

Information on the Whistleblower System for all employees, including temporary workers provided to the employer and external whistleblowers

For the sake of readability and without any intention of discrimination, the male form is exclusively used in the text. This includes all genders.

Under the Whistleblower Protection Act (Whistleblower Protection Act) and the Supply Chain Due Diligence Act (SCDDA), companies are obligated to establish reporting channels for reports/complaints from employees and external individuals regarding violations of regulations.

The Whistleblower Protection Act specifically regulates the protection of natural persons who, in connection with their professional activities or in anticipation of professional activities, have obtained information about violations and report or disclose them to the designated reporting channels (whistleblowers). By making these reports, whistleblowers contribute to preventing, uncovering, and rectifying errors in our company.

Therefore, we encourage you to report suspicious incidents related to or anticipated in the course of your professional activities to our internal reporting channel, providing as specific details as possible. We take the protection of whistleblowers seriously and assure you that you need not fear any retaliatory measures due to or after a legitimate report.

In addition to reporting information about a violation to the internal reporting channel, you may also report it to an external reporting channel. The Whistleblower Protection Act provides for a choice in this regard. However, the Whistleblower Protection Act also indicates that in cases where effective action can be taken internally against the violation and whistleblowers have no reason to fear reprisals, reporting to an internal reporting channel is to be preferred.

Therefore, we ask you to first approach our ombudsman with suspicious incidents.

In accordance with our legal obligation, we provide you with our internal whistleblower system. Through this secure channel, you can report information about violations in the sense of the Whistleblower Protection Act (see "What incidents can be reported?").

Please note: Intentionally false reporting can have criminal consequences.

Internal Reporting System

On our website www.scherdel.com, you will find access to the whistleblower system.

When a report is submitted through the whistleblower system, an IT mechanism is triggered. This mechanism deletes the original email and sends the report without traceability to an external mailbox of the ombudsman. Subsequently, an automatic acknowledgment of receipt is sent to the whistleblower. In addition to the online reporting system, you have the option to contact the ombudsman directly:

ombudsmann@scherdel.com, Phone: +49 9231 603-899.

The ombudsman initiates appropriate follow-up measures. Among other things, he may initiate internal investigations or refer the process for further investigations to a unit responsible for internal investigations within the company or the respective organizational unit, or to a competent authority, as necessary for processing the report. The involved entity processes the report, determines remedial measures, tracks them, and subsequently provides feedback to the ombudsman.

If the original reporter wishes to receive information, they must provide a name and email address and will receive feedback from the ombudsman within 3 months of confirming receipt of the report.

You also have the option to submit reports anonymously. Providing your name is voluntary. However, if you opt for an anonymous report, you will not be informed about any measures that may have been taken.

What incidents can be reported?

You can report information about violations to our ombudsman. Violations include well-founded suspicions or knowledge of actual or potential violations within our company or with another entity with which you have had or currently have professional dealings (e.g., customers and suppliers), whether they have already occurred or are very likely to occur, as well as attempts to conceal such violations.

Violations encompass actions and/or omissions within the scope of professional, entrepreneurial, or official activities that are unlawful and/or abusive and concern regulations or legal areas falling within the substantive scope of the Whistleblower Protection Act (HinSchG). Reports about purely private misconduct that the whistleblower becomes aware of in connection with their professional activities are not protected.

The substantive scope of the Whistleblower Protection Act is regulated in § 2 HinSchG. It includes, among other things, reporting information regarding the following violations:

- Violations punishable by law,
- Violations subject to fines, to the extent that the violated provision serves the protection of life, limb, or health or the protection of the rights of employees or their representative bodies,
- Other violations of federal or state regulations as well as specific directly applicable legal acts of the EU and the European Atomic Energy Community, such as consumer protection, data protection, and environmental protection.

This list is not exhaustive. The legal text of § 2 HinSchG is attached to this letter.

Confidentiality

We handle your personal data and the personal data of the individuals affected by the report confidentially. Personal data is processed in accordance with the provisions of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act. Furthermore, we are obligated under the Whistleblower Protection Act to largely protect the identity of the whistleblower as well as the individuals affected by the report. This means that personal data is only known to the responsible persons of the internal reporting channel and may only be disclosed in legally determined exceptional cases (§ 9 HinSchG).

No disadvantages due to reporting violations

You will not suffer any disadvantages from reporting violations. The Whistleblower Protection Act provides comprehensive protection, which we take very seriously.

Processing of personal data

The internal reporting channel processes personal data of the whistleblower and other persons named in the report in accordance with the legal basis of Art. 6 para. 1 sentence 1(c) GDPR, § 10 HinSchG to the extent necessary for conducting the reporting procedure and appropriate follow-up measures. In particular,

the information provided by you within the whistleblower system is processed for the purpose of verification, for internal investigations (including disclosure to external lawyers, auditors, or other professional practitioners bound by confidentiality obligations, as well as to affected companies of the SCHERDEL Group) and, if necessary, for disclosure to government authorities. The reports are documented in accordance with legal requirements. The documentation is deleted three years after the conclusion of the process.

The documentation may be retained longer to fulfill the requirements of this law or other regulations, as long as this is necessary and proportionate. According to Art. 14 GDPR, you have the right to be informed about the storage, the nature of the data, the purpose of processing, and the identity of the data controller and, if applicable, the whistleblower (if the report was not submitted anonymously) if your data is collected without your knowledge (for example, because you are involved as an accused person in the process of investigating the report). However, if there is a significant risk that such information would jeopardize our ability to effectively investigate the allegation or collect the necessary evidence, this information may be postponed for the period during which this risk exists according to Art. 14 para. 5 sentence 1 lit. b) GDPR. The information must be provided as soon as the reason for the postponement no longer exists.

If you have any questions or concerns, please contact the data protection officer (**Email: datenschutz@scherdel.com / Mobile Phone: +49 1522 6218 309**).

External Reporting Channel of the Federal Government

In addition to internal reporting, the law provides for the possibility of external reporting. For this purpose, the Federal Government establishes an external reporting channel at the Federal Office of Justice (BfJ). The channels for reporting and further information on the external reporting channel of the BfJ are published on the BfJ website.

In addition to the external reporting channel of the BfJ, the existing reporting systems at the Federal Financial Supervisory Authority (BaFin) and the Federal Cartel Office for their specific areas of responsibility are continued. Please also read the information on the websites of these reporting channels/whistleblower channels:

www.bafin.de

www.bundeskartellamt.de

Information on procedures for reporting to European Union (EU) bodies

In addition to information on external reporting procedures under the Whistleblower Protection Act, you can access information on procedures for reporting to EU bodies, institutions, or other entities through the following links. This includes external reporting channels of the Commission, the European Anti-Fraud Office (OLAF), the European Maritime Safety Agency (EMSA), the European Aviation Safety Agency (EASA), the European Securities and Markets Authority (ESMA), and the European Medicines Agency (EMA).

OLAF: https://anti-fraud.ec.europa.eu/index_de

EMSA: <https://www.emsa.europa.eu/de>

EASA: <https://www.easa.europa.eu/en>

ESMA: <https://www.esma.europa.eu/>

EMA: <https://www.ema.europa.eu/en>.

The reporting procedures there remain unaffected by the Whistleblower Protection Act, i.e., they continue unchanged alongside the internal and external reporting procedures under the Whistleblower Protection Act.

Additional information on external reporting channels and procedures of the EU

Further information on external reporting procedures and relevant reporting procedures of organs, institutions, and other entities of the European Union can be found on the website of the Federal Office of Justice (BfJ) at <https://www.bundesjustizamt.de>.

Below you will find a German excerpt from the law, Section 2 Whistleblower Protection Act: Material scope of application.

Gesetzesauszug § 2 HinSchG: Sachlicher Anwendungsbereich:

(1) Dieses Gesetz gilt für die Meldung (§ 3 Absatz 4) und die Offenlegung (§ 3 Absatz 5) von Informationen über

- 1. Verstöße, die strafbewehrt sind,*
- 2. Verstöße, die bußgeldbewehrt sind, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient,*
- 3. sonstige Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union und der Europäischen Atomgemeinschaft*
 - a) zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, unter Einschluss insbesondere des Geldwäschegesetzes und der Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU)Nr. 1781/2006 (ABl. L 141 vom 5.6.2015, S. 1), die durch die Verordnung (EU) 2019/2175 (ABl. L 334 vom 27.12.2019, S. 1) geändert worden ist, in der jeweils geltenden Fassung,*
 - b) mit Vorgaben zur Produktsicherheit und -konformität,*
 - c) mit Vorgaben zur Sicherheit im Straßenverkehr, die das Straßeninfrastruktursicherheitsmanagement, die Sicherheitsanforderungen in Straßentunneln sowie die Zulassung zum Beruf des Güterkraftverkehrsunternehmers oder des Personenkraftverkehrsunternehmers (Kraftomnibusunternehmen) betreffen,*
 - d) mit Vorgaben zur Gewährleistung der Eisenbahnbetriebssicherheit,*
 - e) mit Vorgaben zur Sicherheit im Seeverkehr betreffend Vorschriften der Europäischen Union für die Anerkennung von Schiffsüberprüfungs- und -besichtigungsorganisationen, die Haftung und Versicherung des Beförderers bei der Beförderung von Reisenden auf See, die Zulassung von Schiffsausrüstung, die Seesicherheitsuntersuchung, die Seeleute-Ausbildung, die Registrierung von Personen auf Fahrgastschiffen in der Seeschifffahrt sowie Vorschriften und Verfahrensregeln der Europäischen Union für das sichere Be- und Entladen von Massengutschiffen,*
 - f) mit Vorgaben zur zivilen Luftverkehrssicherheit im Sinne der Abwehr von Gefahren für die betriebliche und technische Sicherheit und im Sinne der Flugsicherung,*
 - g) mit Vorgaben zur sicheren Beförderung gefährlicher Güter auf der Straße, per Eisenbahn und per Binnenschiff,*
 - h) mit Vorgaben zum Umweltschutz,*
 - i) mit Vorgaben zum Strahlenschutz und zur kerntechnischen Sicherheit,*
 - j) zur Förderung der Nutzung von Energie aus erneuerbaren Quellen und der Energieeffizienz,*
 - k) zur Lebensmittel- und Futtermittelsicherheit, zur ökologischen Produktion und zur Kennzeichnung von ökologischen Erzeugnissen, zum Schutz geografischer Angaben für Agrarerzeugnisse und*

Lebensmittel einschließlich Wein, aromatisierter Weinerzeugnisse und Spirituosen sowie garantiert traditioneller Spezialitäten, zum Inverkehrbringen und Verwenden von Pflanzenschutzmitteln sowie zur Tiergesundheit und zum Tierschutz, soweit sie den Schutz von landwirtschaftlichen Nutztieren, den Schutz von Tieren zum Zeitpunkt der Tötung, die Haltung von Wildtieren in Zoos, den Schutz der für wissenschaftliche Zwecke verwendeten Tiere sowie den Transport von Tieren und die damit zusammenhängenden Vorgänge betreffen,

- l) zu Qualitäts- und Sicherheitsstandards für Organe und Substanzen menschlichen Ursprungs, Human- und Tierarzneimittel, Medizinprodukte sowie die grenzüberschreitende Patientenversorgung,*
- m) zur Herstellung, zur Aufmachung und zum Verkauf von Tabakerzeugnissen und verwandten Erzeugnissen,*
- n) zur Regelung der Verbraucherrechte und des Verbraucherschutzes im Zusammenhang mit Verträgen zwischen Unternehmern und Verbrauchern sowie zum Schutz von Verbrauchern im Bereich der Zahlungskonten und Finanzdienstleistungen, bei Preisangaben sowie vor unlauteren geschäftlichen Handlungen,*
- o) zum Schutz der Privatsphäre in der elektronischen Kommunikation, zum Schutz der Vertraulichkeit der Kommunikation, zum Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation, zum Schutz der Privatsphäre der Endeinrichtungen von Nutzern und von in diesen Endeinrichtungen gespeicherten Informationen, zum Schutz vor unzumutbaren Belästigungen durch Werbung mittels Telefonanrufen, automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post sowie über die Rufnummernanzeige und -unterdrückung und zur Aufnahme in Teilnehmerverzeichnisse,*
- p) zum Schutz personenbezogener Daten im Anwendungsbereich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) gemäß deren Artikel 2,*
- q) zur Sicherheit in der Informationstechnik im Sinne des § 2 Absatz 2 des BSI-Gesetzes von Anbietern digitaler Dienste im Sinne des § 2 Absatz 12 des BSI-Gesetzes,*
- r) zur Regelung der Rechte von Aktionären von Aktiengesellschaften,*
- s) zur Abschlussprüfung bei Unternehmen von öffentlichem Interesse nach § 316a Satz 2 des Handelsgesetzbuchs,*
- t) zur Rechnungslegung einschließlich der Buchführung von Unternehmen, die kapitalmarktorientiert im Sinne des § 264d des Handelsgesetzbuchs sind, von Kreditinstituten im Sinne des § 340 Absatz 1 des Handelsgesetzbuchs, Finanzdienstleistungsinstituten im Sinne des § 340 Absatz 4 Satz 1 des Handelsgesetzbuchs, Wertpapierinstituten im Sinne des § 340 Absatz 4a Satz 1 des Handelsgesetzbuchs, Instituten im Sinne des § 340 Absatz 5 Satz 1 des Handelsgesetzbuchs, Versicherungsunternehmen im Sinne des § 341 Absatz 1 des Handelsgesetzbuchs und Pensionsfonds im Sinne des § 341 Absatz 4 Satz 1 des Handelsgesetzbuchs,*
- 4. Verstöße gegen bundesrechtlich und einheitlich geltende Regelungen für Auftraggeber zum Verfahren der Vergabe von öffentlichen Aufträgen und Konzessionen und zum Rechtsschutz in diesen Verfahren ab Erreichen der jeweils maßgeblichen EU-Schwellenwerte,*
- 5. Verstöße, die von § 4d Absatz 1 Satz 1 des Finanzdienstleistungsaufsichtsgesetzes erfasst sind, soweit sich nicht aus § 4 Absatz 1 Satz 1 etwas anderes ergibt,*
- 6. Verstöße gegen für Körperschaften und Personenhandelsgesellschaften geltende steuerliche Rechtsnormen,*
- 7. Verstöße in Form von Vereinbarungen, die darauf abzielen, sich in missbräuchlicher Weise einen steuerlichen Vorteil zu verschaffen, der dem Ziel oder dem Zweck des für Körperschaften und Personenhandelsgesellschaften geltenden Steuerrechts zuwiderläuft,*
- 8. Verstöße gegen Artikel 101 und 102 des Vertrages über die Arbeitsweise der Europäischen Union sowie Verstöße gegen die in § 81 Absatz 2 Nummer 1, 2 Buchstabe a und Nummer 5 sowie Absatz 3 des Gesetzes gegen Wettbewerbsbeschränkungen genannten Rechtsvorschriften.*

9. Verstöße gegen Vorschriften der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1),

10. Äußerungen von Beamtinnen und Beamten, die einen Verstoß gegen die Pflicht zur Verfassungstreue darstellen.

(2) Dieses Gesetz gilt außerdem für die Meldung und Offenlegung von Informationen

über

1. Verstöße gegen den Schutz der finanziellen Interessen der Europäischen Union im Sinne des Artikels 325 des Vertrags über die Arbeitsweise der Europäischen Union

und

2. Verstöße gegen Binnenmarktvorschriften im Sinne des Artikels 26 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union, einschließlich über Absatz 1 Nummer 8 hinausgehender Vorschriften der Europäischen Union über Wettbewerb und staatlichen Beihilfen.